Free Questions for HPE6-A84 by certsinside

Shared by Hancock on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A customer requires a secure solution for connecting remote users to the corporate main site. You are designing a client-to-site virtual private network (VPN) based on Aruba VIA and Aruba Mobility Controllers acting as VPN Concentrators (VPNCs). Remote users will first use the VIA client to contact the VPNCs and obtain connection settings.

The users should only be allowed to receive the settings if they are the customer's "RemoteEmployees" AD group. After receiving the settings, the VIA clients will automatically establish VPN connections, authenticating to CPPM with certificates.

What should you do to help ensure that only authorized users obtain VIA connection settings?

Options:

A- Set up the VPNCs' VIA web authentication profile to use CPPM as the authentication server; set up a service on CPPM that uses AD as the authentication source.

B- Set up the VPNCs' VIA web authentication profile to use an AD domain controller as the LDAP server.

C- Set up the VPNCs' VIA connection profile to use two authentication profiles, one RADIUS profile to CPPM and one LDAP profile to AD.

D- Set up the VPNCs' VIA connection profile to use one authentication profile, which is set to the AD domain controller's hostname.

Answer:

A

Explanation:

The VIA web authentication profile is used to authenticate the users who want to download the VIA connection settings from the VPNCs. The VPNCs can use either an internal database or an external server (such as RADIUS or LDAP) as the authentication source for this profile. To ensure that only authorized users obtain VIA connection settings, you should use CPPM as the external server and configure a service on CPPM that uses AD as the authentication source.This way, you can leverage the role mapping and enforcement features of CPPM to check if the users belong to the ''RemoteEmployees'' AD group and grant or deny them access accordingly1

The other options are not correct because they do not allow you to verify the users' AD group membership before providing them with VIA connection settings. Option B would only check the users' credentials against AD, but not their group membership. Option C would only apply to the VPN connection phase, not the VIA connection settings phase.Option D would not work because the VPNCs do not support LDAP as an authentication source for VIA connection profiles2

1: Configuring the VIA Controller - Aruba, section ''Configuring VIA Web Authentication Profile''2: Configuring VIA Connection Profile - Aruba, section ''Configuring Authentication Profile''

Question 2

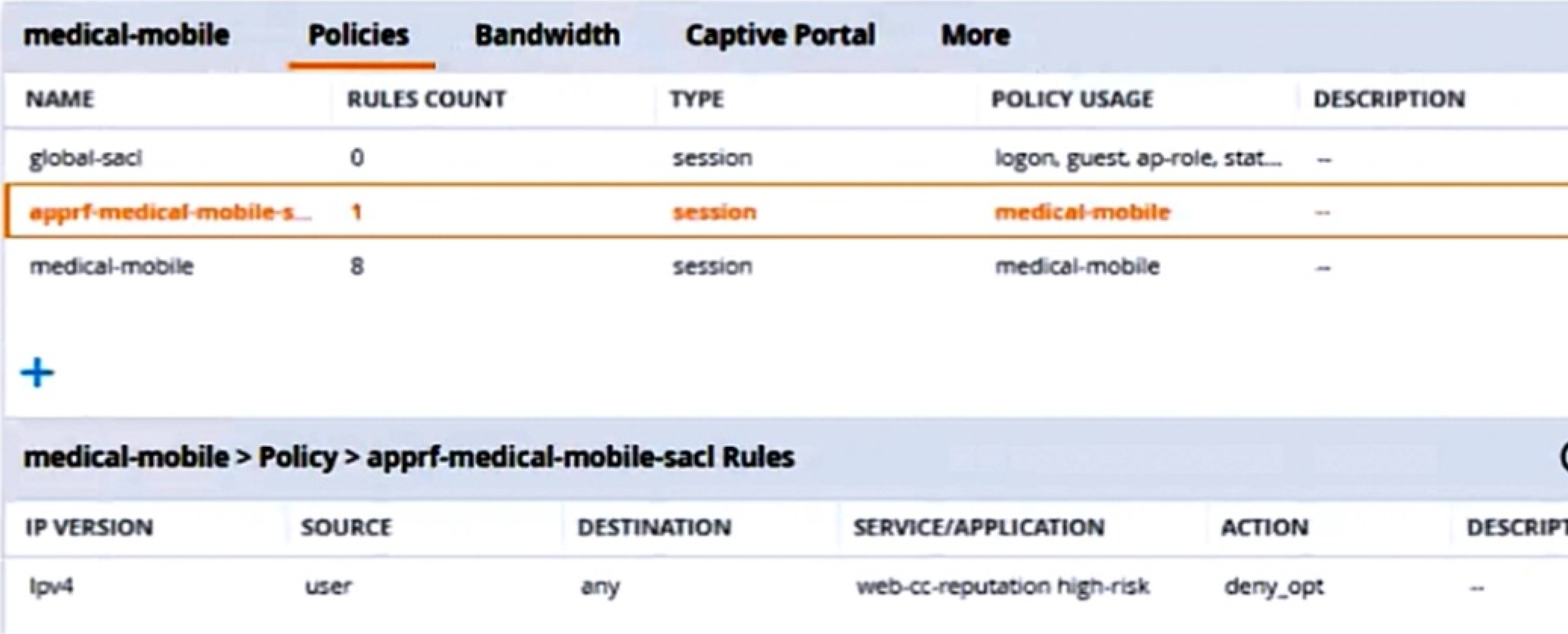
Question Type: MultipleChoice

Refer to the scenario.

A customer requires these rights for clients in the "medical-mobile" AOS firewall role on Aruba Mobility Controllers (MCs):

External devices should not be permitted to initiate sessions with "medical-mobile" clients, only send return traffic.

The line below shows the effective configuration for the role.



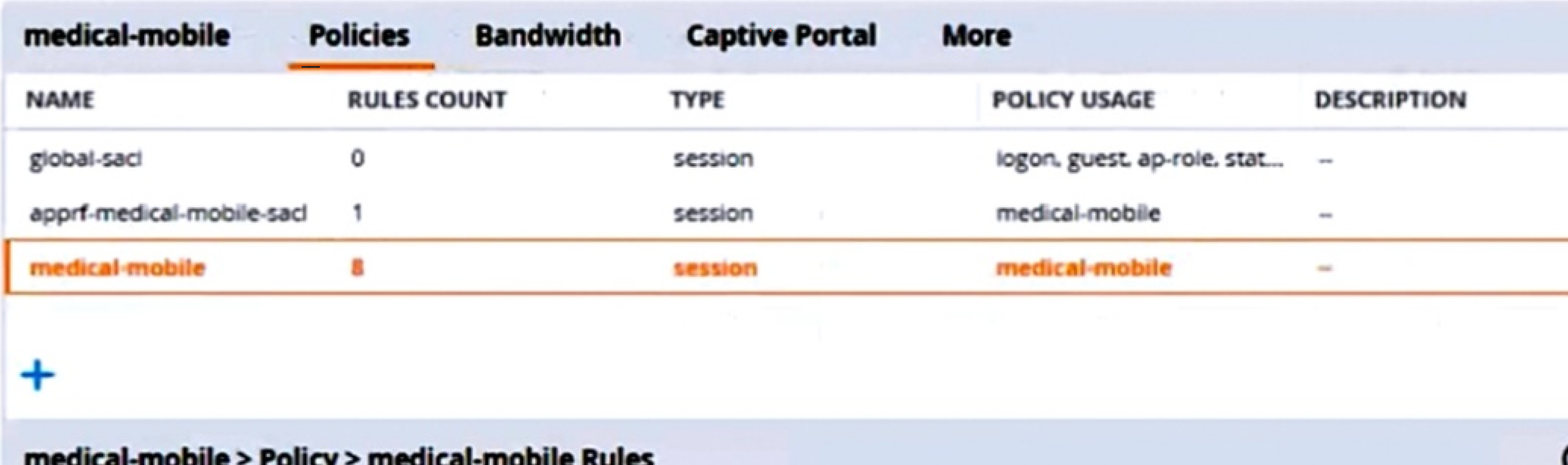
medical-mobile | **Policies** | Bandwidth | Captive Portal | More

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-s...	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

+

medical-mobile > Policy > apprf-medical-mobile-sacl Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPT
Ipv4	user	any	web-cc-reputation high-risk	deny_opt	--



medical-mobile | **Policies** | Bandwidth | Captive Portal | More

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-sacl	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

+

medical-mobile > Policy > medical-mobile Rules

There are multiple issues with this configuration. What is one change you must make to meet the scenario requirements? (In the options, rules in a policy are referenced from top to bottom. For example, ''medical-mobile'' rule 1 is ''ipv4 any any svc-dhcp permit,'' and rule 6 is ''ipv4 any any any permit'.)

Options:

A- Apply the 'apprf-medical-mobile-sjcT policy explicitly to the 'medical-mobile' user-role under the 'medical-mobile' policy.

B- In the 'medical-mobile' policy, change the action for rules 2 and 3 to reject.

C- In the 'medical-mobile' policy, move rule 5 under rule 6.

D- In the 'medical-mobile* policy, change the subnet mask in rule 5 to 255.255.252.0.

Answer:

D

Explanation:

The scenario requires that the clients in the ''medical-mobile'' role are denied access to the 10.1.12.0/22 subnet, which is a range of IP addresses from 10.1.12.0 to 10.1.15.255. However, the current configuration in rule 5 has a subnet mask of 255.255.240.0, which means that it matches any IP address from 10.1.0.0 to 10.1.15.255. This is too broad and would deny access to other subnets in the 10.1.0.0/16 range that should be permitted according to the scenario.Therefore, the subnet mask in rule 5 should be changed to 255.255.252.0, which would match only the IP addresses from 10.1.12.0 to 10.1.15.255 and deny access to them as required by the scenario.1

1: Configuring Firewall Policies - Aruba, section "Firewall Policies"

Question 3

Question Type: **MultipleChoice**

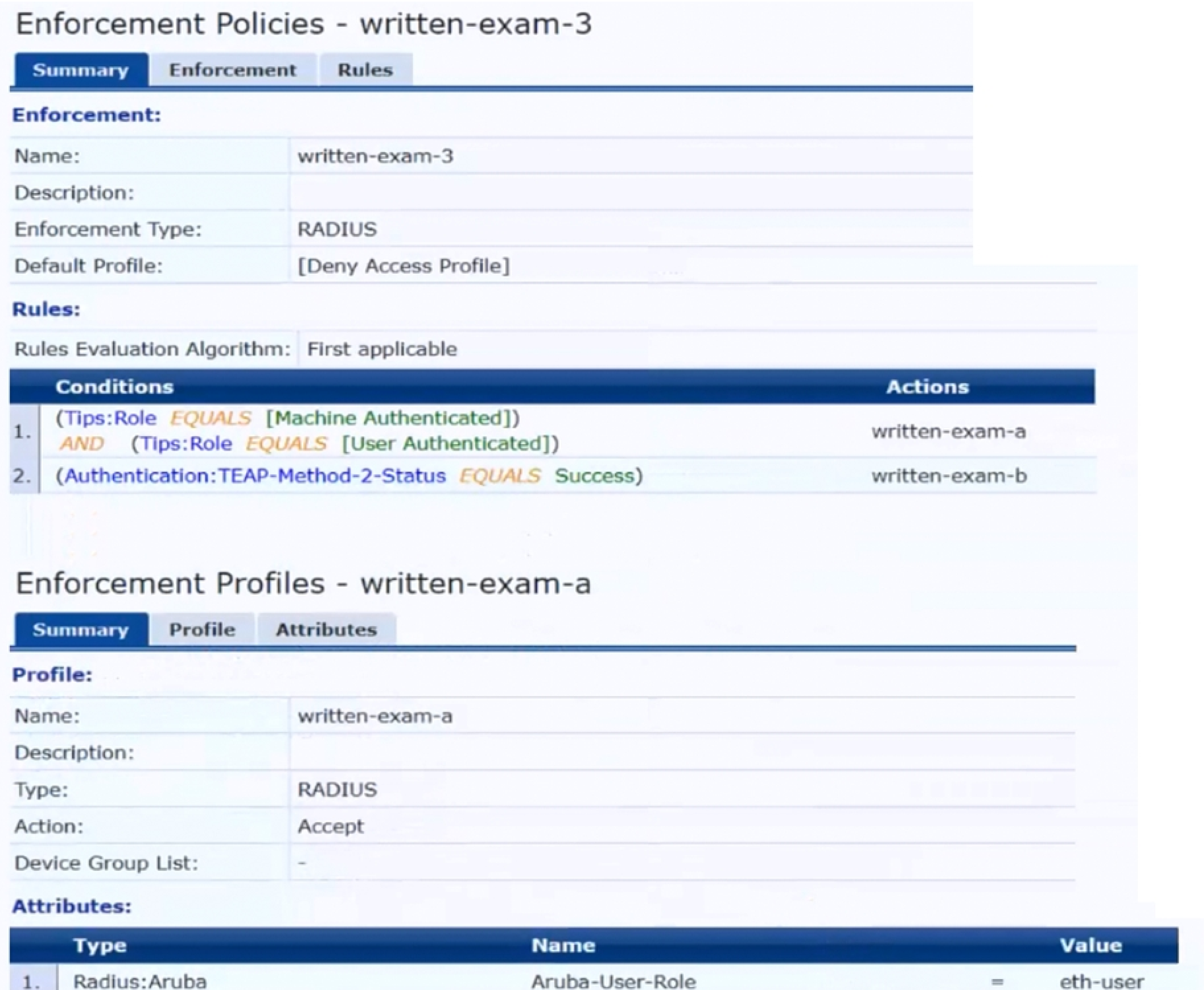
Refer to the scenario.

A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

Switches are using local port-access policies.

The customer wants to start tunneling wired clients that pass user authentication only to an Aruba gateway cluster. The gateway cluster should assign these clients to the "eth-internet" role. The gateway should also handle assigning clients to their VLAN, which is VLAN 20.

The plan for the enforcement policy and profiles is shown below:



Enforcement Policies - written-exam-3

Enforcement:

Name:	written-exam-3
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* [Machine Authenticated]) *AND* (Tips:Role *EQUALS* [User Authenticated])	written-exam-a
2.	(Authentication:TEAP-Method-2-Status *EQUALS* Success)	written-exam-b

Enforcement Profiles - written-exam-a

Profile:

Name:	written-exam-a
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	eth-user

The gateway cluster has two gateways with these IP addresses:

* Gateway 1

o VLAN 4085 (system IP) = 10.20.4.21

o VLAN 20 (users) = 10.20.20.1

o VLAN 4094 (WAN) = 198.51.100.14

* Gateway 2

o VLAN 4085 (system IP) = 10.20.4.22

o VLAN 20 (users) = 10.20.20.2

o VLAN 4094 (WAN) = 198.51.100.12

* VRRP on VLAN 20 = 10.20.20.254

The customer requires high availability for the tunnels between the switches and the gateway cluster. If one gateway falls, the other gateway should take over its tunnels. Also, the switch should be able to discover the gateway cluster regardless of whether one of the gateways is in the cluster.

Assume that you are using the ''myzone'' name for the UBT zone.

Which is a valid minimal configuration for the AOS-CX port-access roles?

Options:

A- port-access role eth-internet gateway-zone zone myzone gateway-role eth-user

B- port-access role internet-only gateway-zone zone myzone gateway-role eth-internet

C- port-access role eth-internet gateway-zone zone myzone gateway-role eth-internet vlan access 20

D- port-access role internet-only gateway-zone zone myzone gateway-role eth-internet vlan access 20

Answer:

B

Explanation:

The UBT solution requires that the edge ports on the switches are configured in VLAN trunk mode, not access mode. This is because the UBT solution uses a special VLAN (VLAN 4095 by default) to encapsulate the user traffic and tunnel it to the gateway. The edge ports need to allow this VLAN as well as any other VLANs that are used for management or control traffic.Therefore, the edge ports should be configured as VLAN trunk ports and allow the necessary VLANs1

1: Aruba Certified Network Technician (ACNT) | HPE Aruba Networking, section "Get the Edge: An Introduction to Aruba Networking Solutions"

Question 4

Question Type: **MultipleChoice**

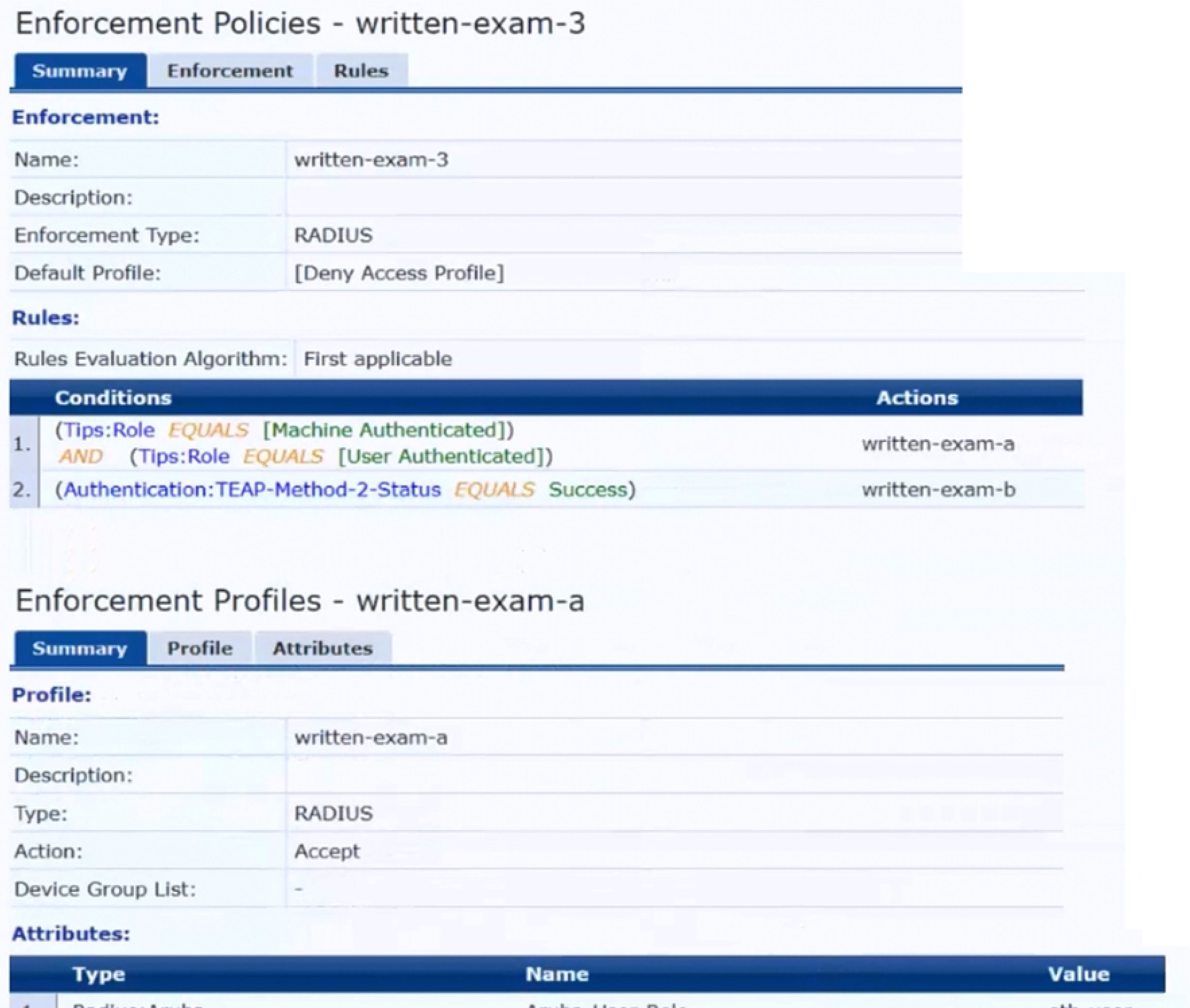
Refer to the scenario.

A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

Switches are using local port-access policies.

The customer wants to start tunneling wired clients that pass user authentication only to an Aruba gateway cluster. The gateway cluster should assign these clients to the ''eth-internet'' role. The gateway should also handle assigning clients to their VLAN, which is VLAN 20.

The plan for the enforcement policy and profiles is shown below:



Enforcement Policies - written-exam-3

Enforcement:

Name:	written-exam-3
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* [Machine Authenticated]) *AND* (Tips:Role *EQUALS* [User Authenticated])	written-exam-a
2.	(Authentication:TEAP-Method-2-Status *EQUALS* Success)	written-exam-b

Enforcement Profiles - written-exam-a

Profile:

Name:	written-exam-a
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name	Value
1.	Radius:Aruba	Aruba-User-Role	eth-user

The gateway cluster has two gateways with these IP addresses:

* Gateway 1

o VLAN 4085 (system IP) = 10.20.4.21

o VLAN 20 (users) = 10.20.20.1

o VLAN 4094 (WAN) = 198.51.100.14

* Gateway 2

o VLAN 4085 (system IP) = 10.20.4.22

o VLAN 20 (users) = 10.20.20.2

o VLAN 4094 (WAN) = 198.51.100.12

* VRRP on VLAN 20 = 10.20.20.254

The customer requires high availability for the tunnels between the switches and the gateway cluster. If one gateway falls, the other gateway should take over its tunnels. Also, the switch should be able to discover the gateway cluster regardless of whether one of the gateways is in the cluster.

What is one change that you should make to the solution?

Options:

A- Change the ubt-client-vlan to VLAN 13.

B- Configure edge ports in VLAN trunk mode.

C- Remove VLAN assignments from role configurations on the gateways.

D- Configure the UBT solution to use VLAN extend mode.

Answer:

C

Explanation:

The UBT solution requires that the VLAN assignments for the wired clients are done by the gateway, not by the switch. Therefore, the role configurations on the gateways should not have any VLAN assignments, as they would override the VLAN 20 that is specified in the enforcement profile. Instead, the role configurations should only have policies that define the access rights for the clients in the ''eth-internet'' role.This way, the gateway can assign the clients to VLAN 20 and apply the appropriate policies based on their role1

1: Aruba Certified Network Technician (ACNT) | HPE Aruba Networking, section ''Get the Edge: An Introduction to Aruba Networking Solutions''

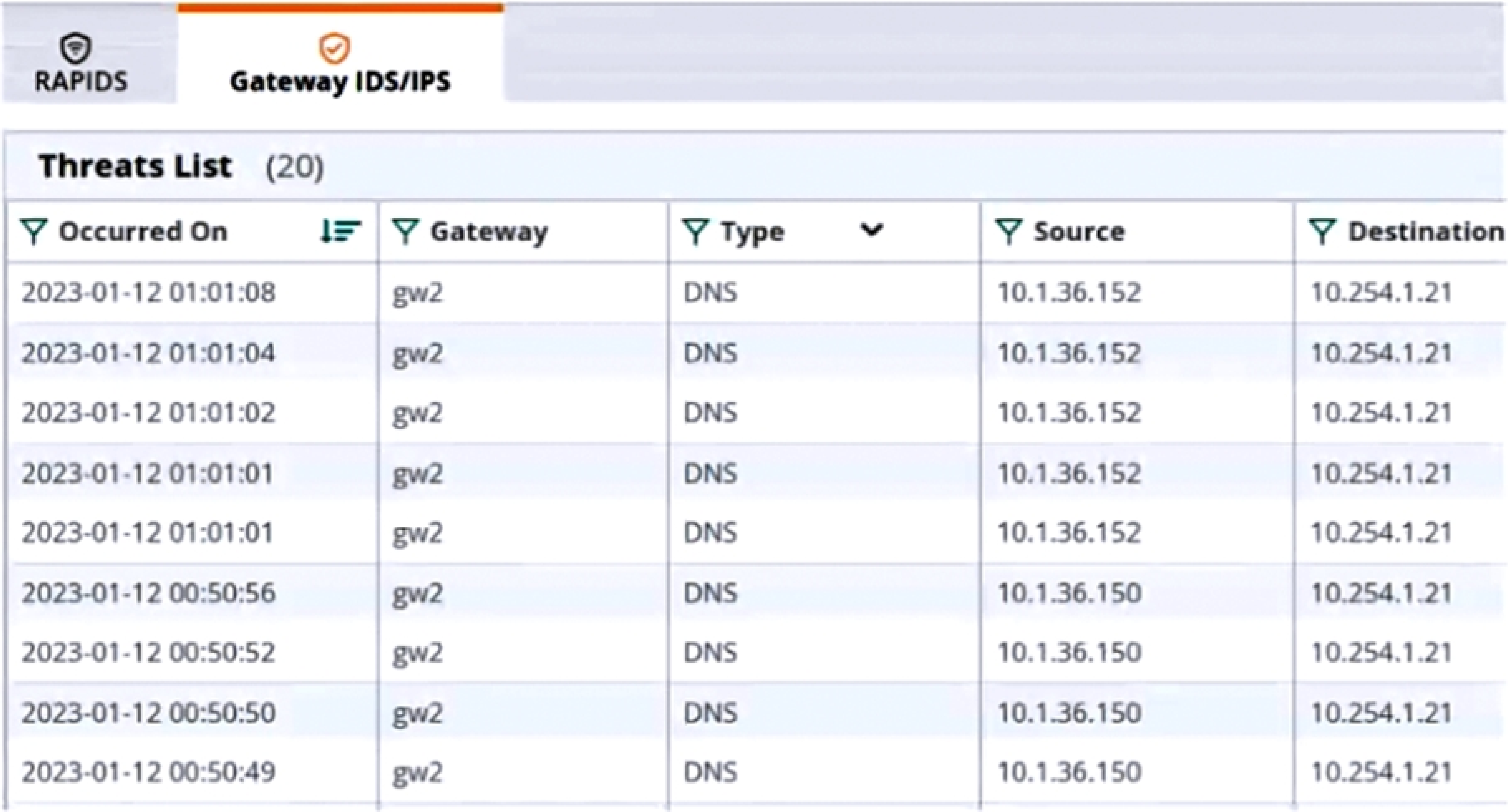
Question 5

Question Type: **MultipleChoice**

Refer to the scenario.

A hospital has an AOS10 architecture that is managed by Aruba Central. The customer has deployed a pair of Aruba 9000 Series gateways with Security licenses at each clinic. The gateways implement IDS/IPS in IDS mode.

The Security Dashboard shows these several recent events with the same signature, as shown below:



Threats List (20)

Occurred On	Gateway	Type	Source	Destination
2023-01-12 01:01:08	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 01:01:04	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 01:01:02	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 01:01:01	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 01:01:01	gw2	DNS	10.1.36.152	10.254.1.21
2023-01-12 00:50:56	gw2	DNS	10.1.36.150	10.254.1.21
2023-01-12 00:50:52	gw2	DNS	10.1.36.150	10.254.1.21
2023-01-12 00:50:50	gw2	DNS	10.1.36.150	10.254.1.21
2023-01-12 00:50:49	gw2	DNS	10.1.36.150	10.254.1.21

Which step could give you valuable context about the incident?

Options:

A- View firewall sessions on the APs and record the threat sources' type and OS.

B- View the user-table on APs and record the threat sources' 802.11 settings.

C- View the RAPIDS Security Dashboard and see if the threat sources are listed as rogues.

D- Find the Central client profile for the threat sources and note their category and family.

Answer:

C

Explanation:

The RAPIDS Security Dashboard is a feature of Aruba Central that provides a comprehensive view of the network security status, including IDS/IPS events, rogue APs, and wireless intrusion detection. By viewing the RAPIDS Security Dashboard, you can see if the threat sources are rogue APs that are spoofing legitimate DNS servers or clients.This can give you valuable context about the incident and help you identify the root cause of the attack1

Question 6

Question Type: MultipleChoice

What is a common characteristic of a beacon between a compromised device and a command and control server?

Options:

A- Use of IPv6 addressing instead of IPv4 addressing

B- Lack of encryption

C- Use of less common protocols such as SNAP

D- Periodic transmission of small, identically sized packets

Answer:

D

Explanation:

A beacon is a type of network traffic that is sent from a compromised device to a command and control (C2) server, which is a remote system that controls the malicious activities of the device . A beacon is used to establish and maintain communication between the device and the C2 server, as well as to receive instructions or exfiltrate data .

A common characteristic of a beacon is that it is periodic, meaning that it is sent at regular intervals, such as every few minutes or hours . This helps the C2 server to monitor the status and availability of the device, as well as to avoid detection by network security tools .

Another common characteristic of a beacon is that it is small and identically sized, meaning that it contains minimal or fixed amount of data, such as a simple acknowledgment or a random string . This helps the device to conserve bandwidth and resources, as well as to avoid detection by network security tools .

Question 7

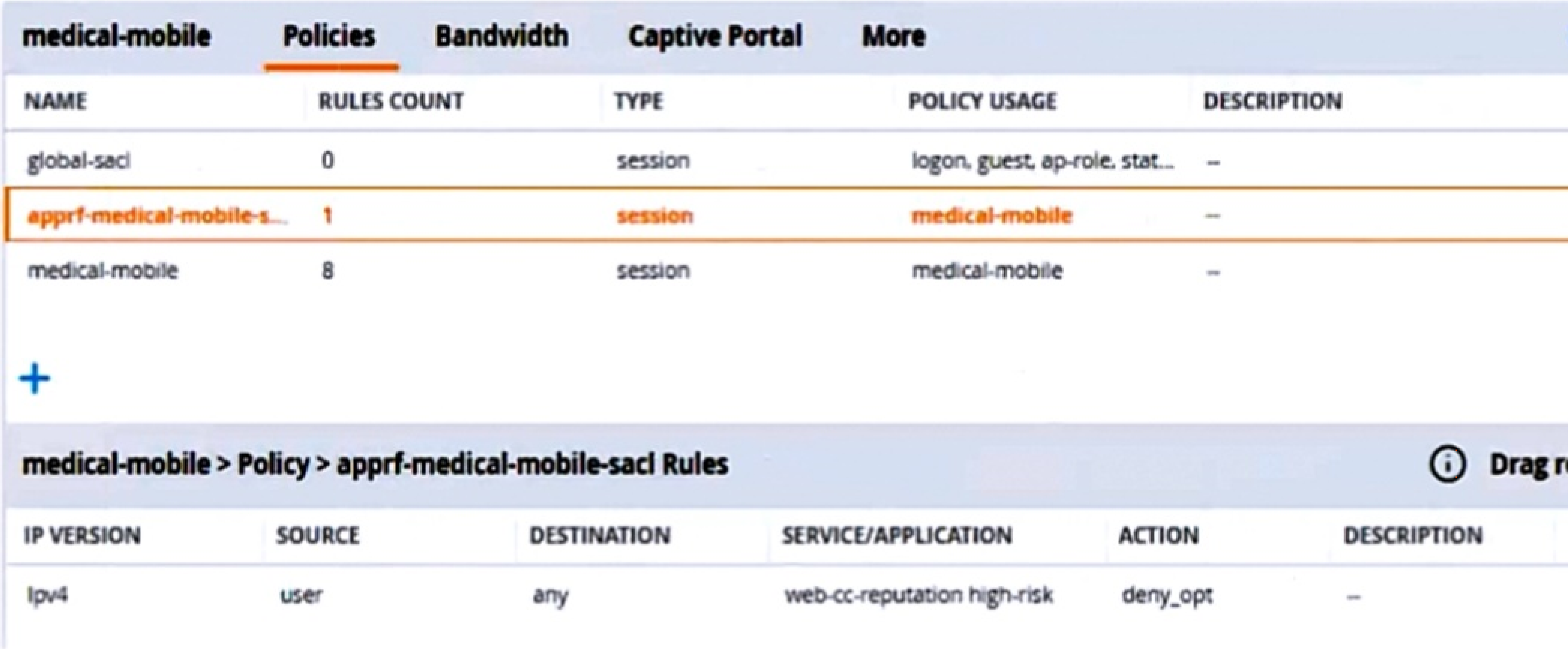
Question Type: **MultipleChoice**

Refer to the scenario.

A customer requires these rights for clients in the "medical-mobile" AOS firewall role on Aruba Mobility Controllers (MCs):

External devices should not be permitted to initiate sessions with "medical-mobile" clients, only send return traffic.

The exhibits below show the configuration for the role.



medical-mobile | Policies | Bandwidth | Captive Portal | More

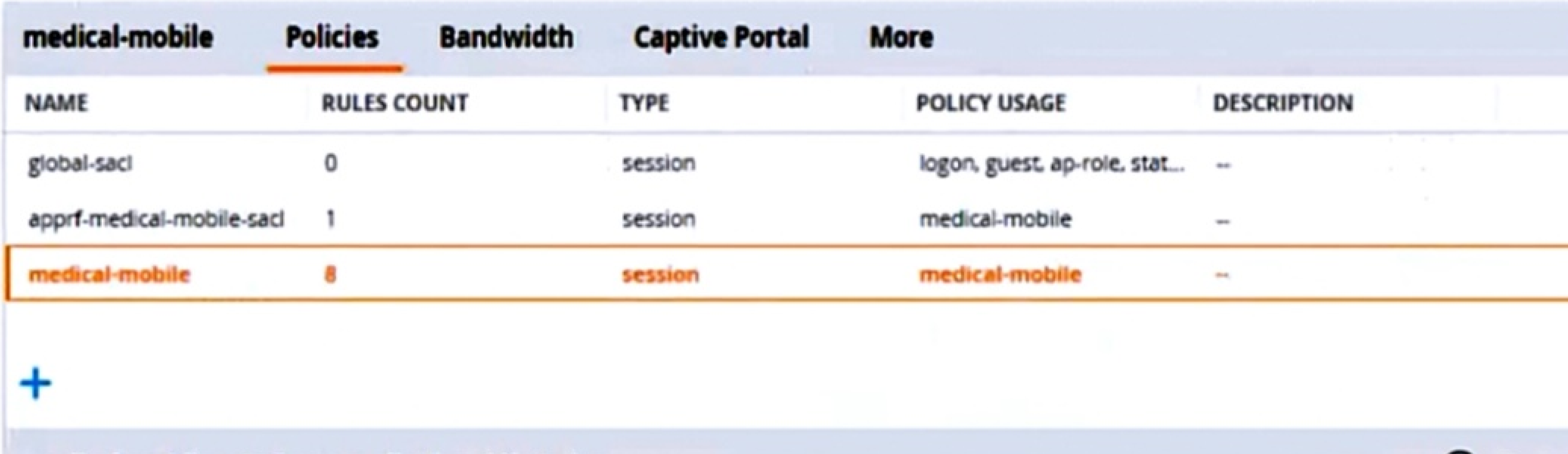
NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-s...	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

+

medical-mobile > Policy > apprf-medical-mobile-sacl Rules

Drag r

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	DESCRIPTION
Ipv4	user	any	web-cc-reputation high-risk	deny_opt	--



medical-mobile | Policies | Bandwidth | Captive Portal | More

NAME	RULES COUNT	TYPE	POLICY USAGE	DESCRIPTION
global-sacl	0	session	logon, guest, ap-role, stat...	--
apprf-medical-mobile-sacl	1	session	medical-mobile	--
medical-mobile	8	session	medical-mobile	--

+

There are multiple issues with the configuration.

What is one of the changes that you must make to the policies to meet the scenario requirements? (In the options, rules in a policy are referenced from top to bottom. For example, ''medical-mobile'' rule 1 is ''ipv4 any any svc-dhcp permit,'' and rule 8 is ''ipv4 any any any permit'.)

Options:

A- In the ''medical-mobile'' policy, change the source in rule 1 to ''user.''

B- In the ''medical-mobile'' policy, change the subnet mask in rule 3 to 255.255.248.0.

C- In the ''medical-mobile'' policy, move rules 6 and 7 to the top of the list.

D- Move the rule in the ''apprf-medical-mobile-sacl'' policy between rules 7 and 8 in the ''medical-mobile'' policy.

Answer:

C

Explanation:

Rules 6 and 7 in the ''medical-mobile'' policy are used to deny access to the WLAN for a period of time if the clients send any SSH or Telnet traffic, as required by the scenario. However, these rules are currently placed below rule 5, which permits access to the Internet for any traffic. This means that rule 5 will override rules 6 and 7, and the clients will not be denied access to the WLAN even if they send

SSH or Telnet traffic.

To fix this issue, rules 6 and 7 should be moved to the top of the list, before rule 5. This way, rules 6 and 7 will take precedence over rule 5, and the clients will be denied access to the WLAN if they send SSH or Telnet traffic, as expected.

Question 8

Question Type: MultipleChoice

Refer to the scenario.

A customer is migrating from on-prem AD to Azure AD as its sole domain solution. The customer also manages both wired and wireless devices with Microsoft Endpoint Manager (Intune).

The customer wants to improve security for the network edge. You are helping the customer design a ClearPass deployment for this purpose. Aruba network devices will authenticate wireless and wired clients to an Aruba ClearPass Policy Manager (CPPM) cluster (which uses version 6.10).

The customer has several requirements for authentication. The clients should only pass EAP-TLS authentication if a query to Azure AD shows that they have accounts in Azure AD. To further refine the clients' privileges, ClearPass also should use information collected by Intune to make access control decisions.

Assume that the Azure AD deployment has the proper prerequisites established.

You are planning the CPPM authentication source that you will reference as the authentication source in 802.1X services.

How should you set up this authentication source?

Options:

A- As Kerberos type

B- As Active Directory type

C- As HTTP type, referencing the Intune extension

D- AS HTTP type, referencing Azure AD's FODN

Answer:

D

Explanation:

An authentication source is a configuration element in CPPM that defines how to connect to an external identity provider and retrieve user or device information . CPPM supports various types of authentication sources, such as Active Directory, LDAP, SQL, Kerberos, and HTTP .

To authenticate wireless and wired clients to Azure AD, you need to set up an authentication source as HTTP type, referencing Azure AD's FQDN . This type of authentication source allows CPPM to use REST API calls to communicate with Azure AD and validate the user or device credentials . You also need to configure the OAuth 2.0 settings for the authentication source, such as the client ID, client secret, token URL, and resource URL .

To use information collected by Intune to make access control decisions, you need to set up another authentication source as HTTP type, referencing the Intune extension . This type of authentication source allows CPPM to use REST API calls to communicate with Intune and retrieve the device compliance status . You also need to configure the OAuth 2.0 settings for the authentication source, such as the client ID, client secret, token URL, and resource URL .

Question 9

Question Type: MultipleChoice

A company has Aruba gateways that are Implementing gateway IDS/IPS in IDS mode. The customer complains that admins are receiving too frequent of repeat email notifications for the same threat. The threat itself might be one that the admins should investigate, but the customer does not want the email notification to repeat as often.

Which setting should you adjust in Aruba Central?

Options:

A- Report scheduling settings

B- Alert duration and threshold settings

C- The IDS policy setting (strict, medium, or lenient)

D- The allowlist settings in the IDS policy

Answer:

B

Explanation:

Alert duration and threshold settings are used to control how often and under what conditions email notifications are sent for gateway IDS/IPS events1. By adjusting these settings, the customer can reduce the frequency of repeat email notifications for the same threat, while still being informed of any critical or new threats.

To adjust the alert duration and threshold settings in Aruba Central, the customer can follow these steps1:

In the Aruba Central app, set the filter to Global, a group, or a device.

Under Analyze, click Alerts & Events.

Click the Config icon to open the Alert Severities & Notifications page.

Select the Gateway IDS/IPS tab to view the alert categories and severities for gateway IDS/IPS events.

Click on an alert category to expand it and view the alert duration and threshold settings for each severity level.

Enter a value in minutes for the alert duration. This is the time period during which the alert is active and email notifications are sent.

Enter a value for the alert threshold. This is the number of times the alert must be triggered within the alert duration before an email notification is sent.

Click Save.

By increasing the alert duration and/or threshold values, the customer can reduce the number of email notifications for recurring threats, as they will only be sent when the threshold is reached within the duration. For example, if the customer sets the alert duration to 60 minutes and the alert threshold to 10 for a Critical severity level, then an email notification will only be sent if the same threat occurs 10 times or more within an hour.

Question 10

Question Type: MultipleChoice

A company has Aruba gateways and wants to start implementing gateway IDS/IPS. The customer has selected Block for the Fail Strategy.

What might you recommend to help minimize unexpected outages caused by using this particular fall strategy?

Options:

A- Configuring a relatively high threshold for the gateway threat count alerts

B- Making sure that the gateways have formed a cluster and operate in default gateway mode

C- Setting the IDS or IPS policy to the least restrictive option, Lenient

D- Enabling alerts and email notifications for events related to gateway IPS engine utilization and errors

Answer:

D

Explanation:

The correct answer is D. Enabling alerts and email notifications for events related to gateway IPS engine utilization and errors.

Gateway IDS/IPS is a feature that allows the Aruba gateways to monitor and block malicious or unwanted traffic based on predefined or custom rules 1. The Fail Strategy is a setting that determines how the gateways handle traffic when the IPS engine fails or crashes 2. The Block option means that the gateways will stop forwarding traffic until the IPS engine recovers, while the Bypass option means that the gateways will continue forwarding traffic without inspection 2.

The Block option provides more security, but it also increases the risk of network outages if the IPS engine fails frequently or for a long time 2. To minimize this risk, it is recommended to enable alerts and email notifications for events related to gateway IPS engine utilization and errors 3. This way, the network administrators can be informed of any issues with the IPS engine and take appropriate actions to restore or troubleshoot it 3.

The other options are not correct or relevant for this issue:

Option A is not correct because configuring a relatively high threshold for the gateway threat count alerts would not help minimize unexpected outages caused by using the Block option. The gateway threat count alerts are used to notify the network administrators of the number of threats detected by the IPS engine, but they do not affect how the gateways handle traffic when the IPS engine fails 4.

Option B is not correct because making sure that the gateways have formed a cluster and operate in default gateway mode would not help minimize unexpected outages caused by using the Block option. The gateway cluster mode is used to provide high availability and load balancing for the gateways, but it does not affect how the gateways handle traffic when the IPS engine fails . The default gateway mode is used to enable routing and NAT functions on the gateways, but it does not affect how the gateways handle traffic when the IPS engine fails .

Option C is not correct because setting the IDS or IPS policy to the least restrictive option, Lenient, would not help minimize unexpected outages caused by using the Block option. The IDS or IPS policy is used to define what rules are applied by the IPS engine to inspect and block traffic, but it does not affect how the gateways handle traffic when the IPS engine fails 2. The Lenient option contains fewer and older rules than the Moderate or Strict options, which means that it provides less security and more false negatives .

Question 11

Question Type: **MultipleChoice**

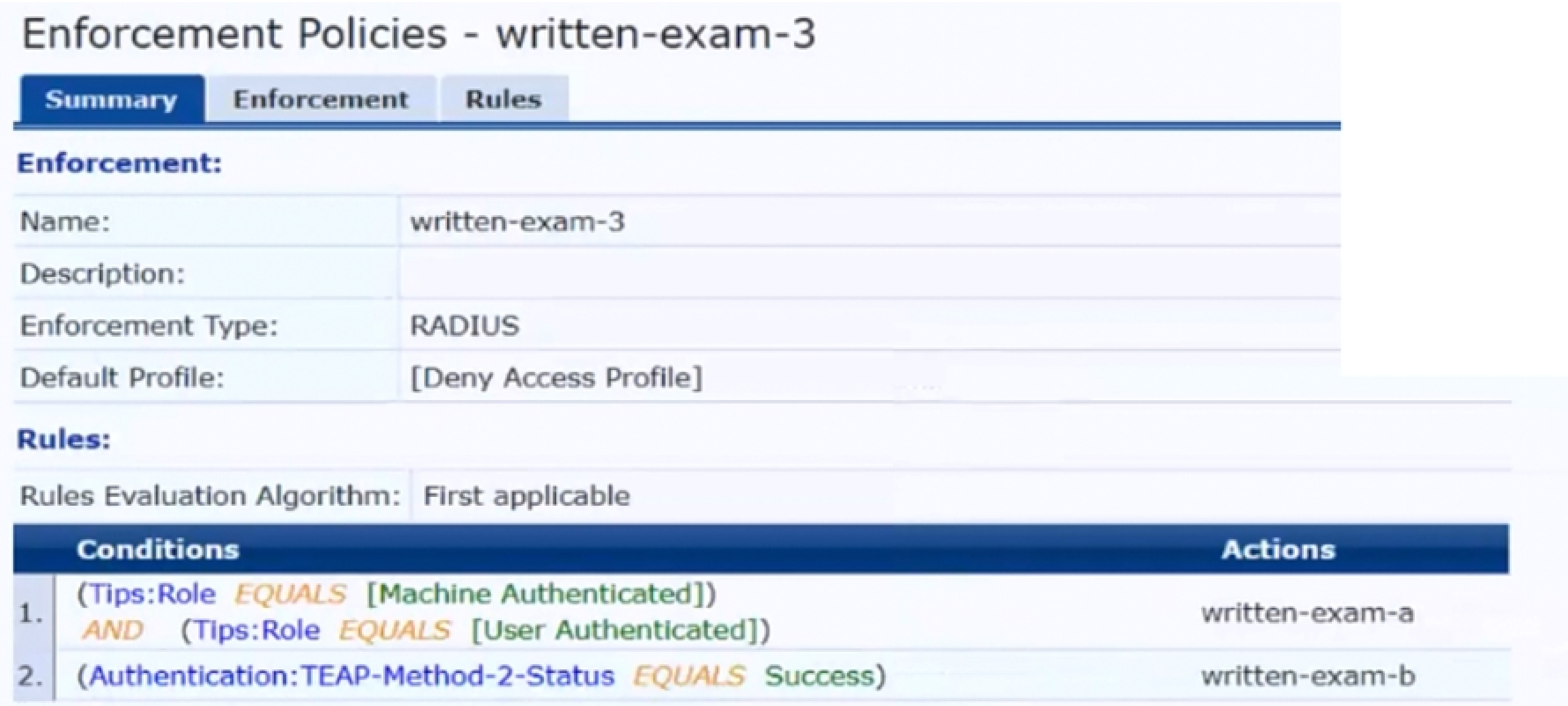
Refer to the scenario.

A customer has an Aruba ClearPass cluster. The customer has AOS-CX switches that implement 802.1X authentication to ClearPass Policy Manager (CPPM).

Switches are using local port-access policies.

The customer wants to start tunneling wired clients that pass user authentication only to an Aruba gateway cluster. The gateway cluster should assign these clients to the "eth-internet" role. The gateway should also handle assigning clients to their VLAN, which is VLAN 20.

The plan for the enforcement policy and profiles is shown below:



Enforcement Policies - written-exam-3

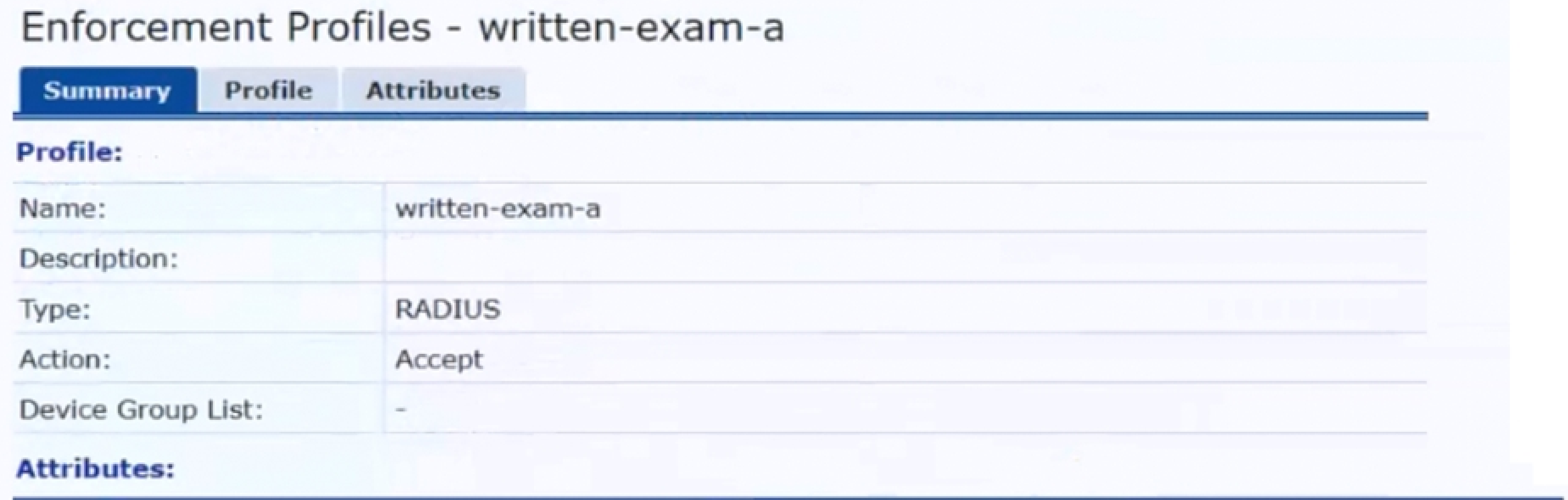
Enforcement:

Name:	written-exam-3
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* [Machine Authenticated]) *AND* (Tips:Role *EQUALS* [User Authenticated])	written-exam-a
2.	(Authentication:TEAP-Method-2-Status *EQUALS* Success)	written-exam-b



Enforcement Profiles - written-exam-a

Profile:

Name:	written-exam-a
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

The gateway cluster has two gateways with these IP addresses:

* Gateway 1

o VLAN 4085 (system IP) = 10.20.4.21

o VLAN 20 (users) = 10.20.20.1

o VLAN 4094 (WAN) = 198.51.100.14

* Gateway 2

o VLAN 4085 (system IP) = 10.20.4.22

o VLAN 20 (users) = 10.20.20.2

o VLAN 4094 (WAN) = 198.51.100.12

* VRRP on VLAN 20 = 10.20.20.254

The customer requires high availability for the tunnels between the switches and the gateway cluster. If one gateway falls, the other gateway should take over its tunnels. Also, the switch should be able to discover the gateway cluster regardless of whether one of the gateways is in the cluster.

Assume that you have configured the correct UBT zone and port-access role settings. However, the solution is not working.

What else should you make sure to do?

Options:

A- Assign VLAN 20 as the access VLAN on any edge ports to which tunneled clients might connect.

B- Create a new VLAN on the AOS-CX switch and configure that VLAN as the UBT client VLAN.

C- Assign sufficient VIA licenses to the gateways based on the number of wired clients that will connect.

D- Change the port-access auth-mode mode to client-mode on any edge ports to which tunneled clients might connect.

Answer:

B

Explanation:

The correct answer is B. Create a new VLAN on the AOS-CX switch and configure that VLAN as the UBT client VLAN.

User-based tunneling (UBT) is a feature that allows the AOS-CX switches to tunnel the traffic from wired clients to a mobility gateway cluster, where they can be assigned a role and a VLAN based on their authentication and authorization 1. To enable UBT, the switches need to have a UBT zone configured with the IP addresses of the gateways, and a UBT client VLAN configured with the ubt-client-vlan command 2.

The UBT client VLAN is a special VLAN that is used to encapsulate the traffic from the tunneled clients before sending it to the gateways. The UBT client VLAN must be different from any other VLANs used on the switch or the network, and it must not be assigned to any ports or interfaces on the switch 2. The UBT client VLAN is only used internally by the switch for UBT, and it is not visible to the clients or the gateways.

In this scenario, the customer wants to tunnel the clients that pass user authentication to the gateway cluster, where they will be assigned to VLAN 20. Therefore, the switch must have a UBT client VLAN configured that is different from VLAN 20 or any other VLANs on the network. For example, the switch can use VLAN 4000 as the UBT client VLAN, as shown in one of the web search results 3. The switch must also have a UBT zone configured with the system IP addresses of the gateways as the primary and backup controllers, as explained in question 3.

The other options are not correct or relevant for this issue:

Option A is not correct because assigning VLAN 20 as the access VLAN on any edge ports to which tunneled clients might connect would conflict with UBT. The access VLAN is the VLAN that is assigned to untagged traffic on a port, and it is used for local switching on the switch 4. If VLAN 20 is assigned as the access VLAN, then the traffic from the clients will not be tunneled to the gateways, but rather switched locally on VLAN 20. This would defeat the purpose of UBT and cause inconsistency in role and VLAN assignment.

Option C is not correct because VIA licenses are not required for UBT. VIA licenses are required for enabling VPN services on Aruba Mobility Controllers for remote access clients using Aruba Virtual Intranet Access (VIA) software . VIA licenses are not related to UBT or wired clients.

Option D is not correct because changing the port-access auth-mode mode to client-mode on any edge ports to which tunneled clients might connect would not affect UBT. The port-access auth-mode mode determines how a port handles authentication requests from multiple clients connected to a single port . Client-mode is the default mode that allows only one client per port, while multi-client-mode allows multiple clients per port. The port-access auth-mode mode does not affect how UBT works or how traffic is tunneled from a port.